MÁSTER SEGURIDAD INFORMÁTICA

OBJETIVOS Y COMPETENCIAS

Objetivos

El objetivo general del máster es preparar al estudiante para el ejercicio de las funciones de experto en seguridad.

Todo el proceso formativo está dirigido a que los alumnos del Máster adquieran las competencias que se recogen en este apartado y estará presidido de manera real y efectiva por los siguientes principios informadores:

a. El respeto y la subordinación de toda actuación a los derechos fundamentales de la persona por su carácter de absolutos axiológicos.

b. La subordinación al principio de igualdad, con especial atención a la no discriminación por razón de sexo, de conformidad con lo previsto en el artículo 14 de la Constitución.

c. El fomento del principio de igualdad de oportunidades en lo que comporta de exigencia de implementación de acciones de discriminación positiva respecto a las personas con diversidad de capacidades.

d. El fomento de la estima de la paz, el pluralismo, el respeto a la diferencia y de los demás valores convivenciales propios de una sociedad democrática avanzada.

Los objetivos generales de nuestra propuesta, de conformidad con el Marco Español Cualificaciones para la Educación Superior (MECES) son:

1	Conocer y comprender la legislación dirigida a la protección de bienes informáticos, sistemas de información, así como en el despliegue de su actividad, en especial la regulación penal de los comportamientos delictivos asociados.
2	Analizar riesgos legales relacionados con la seguridad en todo tipo de sistemas.
3	Conocer y saber aplicar procesos de gestión y mejora de la seguridad en las organizaciones.
4	Conocer y saber aplicar los principales estándares y buenas prácticas de auditoría de la seguridad.
5	Comprender y saber valorar los diferentes algoritmos y técnicas criptográficas, y los mecanismos de protección asociados a ellas.
6	Conocer las plataformas hardware especializadas para la seguridad informática.
7	Entender el concepto de vulnerabilidad y su tipología y saber analizar vulnerabilidades en sistemas concretos.
8	Conocer las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes, el software de aplicación, los sistemas Web y las bases de datos.
9	Conocer y saber aplicar correctamente las principales técnicas de análisis forense.

Competencias generales

Con el fin de cumplir los objetivos del Máster, los estudiantes desarrollarán las competencias generales, indicadas a continuación:

1. Aplicar los conocimientos adquiridos y ser capaces de resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con el área de la seguridad informática.

2. Integrar conocimientos para formular juicios a partir de determinada información. A la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios en materia de asesoramiento en seguridad informática.

3. Mantener una actitud que les permita estudiar de manera autónoma y promover la formación continua en su futuro desempeño profesional como experto en seguridad informática.

4. Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno seguridad informática, e implementarlos y desarrollarlos mediante los métodos y procesos adecuados.

5. Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática, en el seno de las entidades de TI.

6. Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la revisión del propio progreso y desempeño en la seguridad informática.

7. Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes.

8. Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente.

9. Manejar adecuadamente información relativa al sector de la seguridad informática. Atendiendo a la legislación vigente, notas técnicas, revistas especializadas, Internet, documentos internos de la empresa, etc.

Competencias específicas

10. Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.

11. Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.

12. Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.

13. Asesorar sobre el cumplimiento de la legislación reguladora de la protección de datos en materia de seguridad, en especial sobre la adopción de las medidas de índole técnica y organizativas necesarias

14. Discernir sobre los distintos entornos de seguridad existentes para poder seleccionar el óptimo siguiendo una razonamiento profesional y completa.

15. Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.

16. Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.

17. Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.

18. Comprender el funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.

19. Diseñar un plan de seguridad adaptado a las necesidades del entorno y a su perfil de riesgos.

20. Conocer todos los activos del negocio de la empresa y las variables necesarias para poder implementar un SGSI.

21. Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.

22. Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.

23. Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.

24. Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.

25. Conocer y comprender la legislación europea en materia de seguridad, para poder emitir juicios sobre su aplicabilidad y relevancia en cada ámbito.

26. Discernir los distintos mecanismos criptográficos para seleccionar el óptimo en cada ámbito de aplicación.

27. Optimizar las políticas de seguridad de la infraestructura de red de la entidad.

28. Proteger la integridad de la bases de datos para asegurar la confidencialidad de la información sensible contenida.

29. Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.

30. Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas.

31. Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante desastres.

32. Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.

33. Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.

34. Conocer e interpretar normativa de centros de respuesta a incidentes de seguridad, seguridad en centros financieros, seguridad en infraestructuras de defensa y principales conceptos de auditoría de sistemas.

35. Implantar procesos de análisis forense de cualquier sistema informático.

36. Diseñar, implantar e institucionalizar un proceso de gestión de riesgos legales en cualquier organización.

Competencias transversales

1. Capacidad de innovación y flexibilidad en entornos nuevos de aprendizaje como es la enseñanza on-line.
2. Conocer, y utilizar con habilidad, los mecanismos básicos de uso de comunicación bidireccional entre profesores y alumnos, foros, chats, etc.
3. Utilizar las herramientas para presentar, producir y comprender la información que les permita transformarla en conocimiento.
4. Capacidad para realizar una enseñanza personalizada adaptada al espacio (aula virtual multicultural y multirracial) a los recursos y a las situaciones y necesidades personales de los alumnos.
5. Capacidad de Investigar y comunicar los resultados de la investigación.